

(Translation)

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: July 17, 2001  
Application Number: No. 2001-216704  
Applicant: FDK Corporation

Date: August 7, 2003  
Commissioner, Patent Office Yasuo IMAI (Seal)

Certificate No. 2003-3063565

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 1 年   7 月 1 7 日  
Date of Application:

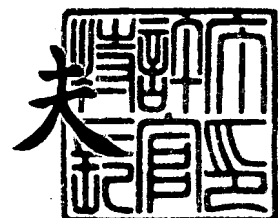
出 願 番 号            特 願 2 0 0 1 - 2 1 6 7 0 4  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 1 - 2 1 6 7 0 4 ]

願            人            エフ・ディー・ケイ株式会社  
Applicant(s):

2 0 0 3 年   8 月   7 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫





【書類名】 特許願

【整理番号】 IP01397

【あて先】 特許庁長官 殿

【国際特許分類】 H03K 3/84

【発明者】

    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

    【氏名】 山本 博康

【発明者】

    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

    【氏名】 志賀 隆明

【発明者】

    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

    【氏名】 清水 隆邦

【発明者】

    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

    【氏名】 鯉渕 美佐子

【特許出願人】

    【識別番号】 390022792

    【氏名又は名称】 いわき電子株式会社

【代理人】

    【識別番号】 100067046

    【弁理士】

    【氏名又は名称】 尾股 行雄

    【電話番号】 03-3543-0036

**【選任した代理人】****【識別番号】** 100096862**【弁理士】****【氏名又は名称】** 清水 千春**【電話番号】** 03-3543-0036**【手数料の表示】****【予納台帳番号】** 008800**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置

【特許請求の範囲】

【請求項 1】 乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、

一定回数を計数する第1のカウンター（3）と、前記乱数発生器から出力された乱数データの出現回数を計数して回数データを生成する第2のカウンター（4）とを備え、

第1のカウンターで計数された周期ごとに第2のカウンターの回数データを保持するレジスター（5）を備え、

このレジスターに保持された回数データを検証データとして出力する出力回路（6）を備えたことを特徴とする1ビット乱数発生装置。

【請求項 2】 出力回路（6）に代えて、

予め設定された上限比較データおよび下限比較データとレジスター（5）に保持されたデータとを比較して検証信号を出力する比較器（7）を備えたことを特徴とする請求項1に記載の1ビット乱数発生装置。

【請求項 3】 乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、

この乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、

前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器（9）を備え、

前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアするカウンター（10）を備え、

このカウンターに保持されたデータを検証データとして出力する出力回路（6）

）を備えたことを特徴とする 1 ビット乱数発生装置。

【請求項 4】 乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、

この乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、

前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する第 1 の比較器（11）を備え、

第 1 の比較器からカウントアップ信号を受けたときにカウントアップするとともに、第 1 の比較器からカウントクリア信号を受けたときにカウントクリアするカウンタ（10）を備え、

このカウンタの出力データを保持するレジスタ（12）を備え、

このレジスタのデータと前記カウンタの出力データとを比較して、前者より後者の方が大きいときにデータ上書き信号を出力するとともに、それ以外の場合にデータ保持信号を出力する第 2 の比較器（13）を備え、

第 2 の比較器からデータ上書き信号を受けたときに前記カウンタの出力データを前記レジスタに書き込むとともに、第 2 の比較器からデータ保持信号を受けたときに前記レジスタのデータを保持するように制御する制御回路（14）を備え、

前記レジスタに保持されたデータを検証データとして出力する出力回路（15）を備えたことを特徴とする 1 ビット乱数発生装置。

【請求項 5】 出力回路（15）に代えて、

予め設定された比較データとレジスタ（12）に保持されたデータとを比較して検証信号を出力する第 3 の比較器（16）を備えたことを特徴とする請求項 4 に記載の 1 ビット乱数発生装置。

【請求項 6】 乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、

一定回数を計数する第 1 のカウンタ（17）を備え、

前記乱数発生器から出力された前回の乱数データを保持するデータ保持器（８）を備え、

前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器（９）を備え、

前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアする第２のカウンタ（１８）を備え、

第２のカウンタの出力データをデコードして各信号長ごとに出力するデコーダ（１９）を備え、

このデコーダの出力データを各信号長ごとにそれぞれカウントする複数個の第３のカウンタ（２０）を備え、

第１のカウンタで計数された一定回数ごとに第３の各カウンタの出力データをそれぞれ保持する複数個のレジスタ（２１）を備え、

第１のカウンタで計数された一定回数ごとの信号と前記比較器の出力データとに基づいて前記各レジスタから検証データを出力するように制御する制御回路（２２）を備えたことを特徴とする１ビット乱数発生装置。

【請求項７】 レジスタ（２１）の出力データを選択して出力する選択回路（２３）を付設したことを特徴とする請求項６に記載の１ビット乱数発生装置。

【請求項８】 請求項１または請求項３または請求項４または請求項６または請求項７に記載の１ビット乱数発生装置（１）を複数個並列に接続し、

これら１ビット乱数発生装置から出力された検証データをビットごとに選択して出力する選択回路（２６）を付設したことを特徴とする多数ビット乱数発生装置。

【請求項９】 請求項２または請求項５に記載の１ビット乱数発生装置（２４）を複数個並列に接続し、

これら１ビット乱数発生装置から出力された検証信号をビットごとに選択して出力する選択回路（２７）を付設したことを特徴とする多数ビット乱数発生装置

。

【請求項 10】 請求項 1 から請求項 7 までのいずれかに記載の 1 ビット乱数発生装置（1、24）を有し、

この 1 ビット乱数発生装置から出力された乱数データをシリアルデータからパラレルデータへ変換するシフトレジスター（31）を備え、

一定のパラレルデータのビット長を計数するカウンタ（32）を備え、

このカウンタで計数された周期ごとに前記シフトレジスターのパラレルデータを保持するレジスター（33）を備え、

予め設定された確率上限データおよび確率下限データと前記レジスターに保持されたパラレルデータとを比較して確率信号を出力する比較器（34）を備えたことを特徴とする確率発生装置。

【請求項 11】 請求項 8 または請求項 9 に記載の多数ビット乱数発生装置（25）を有し、

予め設定された確率上限データおよび確率下限データと前記多数ビット乱数発生装置から出力された乱数データとを比較して確率信号を出力する比較器（35）を備えたことを特徴とする確率発生装置。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、科学技術計算、ゲーム機、或いは暗号化処理などに利用するに好適な 1 ビット乱数発生装置および多数ビット乱数発生装置と、これらを用いた確率発生装置に関するものである。

##### 【0002】

##### 【従来の技術】

一般に、乱数発生器を備えた乱数発生装置（1 ビット乱数発生装置、多数ビット乱数発生装置）や確率発生装置において、その製品としての信頼性を高めるためには、乱数発生器から送出される乱数データに前後関係、規則性、周期性がないことに加えて、この乱数データに出現一様性（乱数によって出現率に差異が生じないこと）があることが重要となる。そのため従来は、乱数発生器から連続的



に送出された膨大の乱数データを使用者が統計処理してその出現一様性を検証していた。

#### 【0003】

##### 【発明が解決しようとする課題】

しかし、これでは乱数データの統計処理が面倒で煩雑となるので、出現一様性の検証に手間がかかるという不都合があった。

#### 【0004】

本発明は、このような事情に鑑み、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置を提供することを目的とする。

#### 【0005】

##### 【課題を解決するための手段】

本発明では、1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置の製品としての信頼性を高めるべく、乱数データの出現一様性を自ら検証できる機能を内蔵することに着目した。

#### 【0006】

すなわち、本発明のうち請求項1に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、一定回数を計数する第1のカウンタ(3)と、前記乱数発生器から出力された乱数データの出現回数を計数して回数データを生成する第2のカウンタ(4)とを備え、第1のカウンタで計数された周期ごとに第2のカウンタの回数データを保持するレジスタ(5)を備え、このレジスタに保持された回数データを検証データとして出力する出力回路(6)を備えて構成される。

#### 【0007】

また、本発明のうち請求項2に係る発明は、上記出力回路(6)に代えて、予め設定された上限比較データおよび下限比較データと上記レジスタ(5)に保持されたデータとを比較して検証信号を出力する比較器(7)を備えて構成される。

#### 【0008】

また、本発明のうち請求項 3 に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器（9）を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアするカウンタ（10）を備え、このカウンタに保持されたデータを検証データとして出力する出力回路（6）を備えて構成される。

#### 【0009】

また、本発明のうち請求項 4 に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する第 1 の比較器（11）を備え、第 1 の比較器からカウントアップ信号を受けたときにカウントアップするとともに、第 1 の比較器からカウントクリア信号を受けたときにカウントクリアするカウンタ（10）を備え、このカウンタの出力データを保持するレジスタ（12）を備え、このレジスタのデータと前記カウンタの出力データとを比較して、前者より後者の方が大きいときにデータ上書き信号を出力するとともに、それ以外の場合にデータ保持信号を出力する第 2 の比較器（13）を備え、第 2 の比較器からデータ上書き信号を受けたときに前記カウンタの出力データを前記レジスタに書き込むとともに、第 2 の比較器からデータ保持信号を受けたときに前記レジスタのデータを保持するように制御する制御回路（14）を備え、前記レジスタに保持されたデータを検証データとして出力する出力回路（15）を備えて構成される。

#### 【0010】

また、本発明のうち請求項 5 に係る発明は、上記出力回路（15）に代えて、予め設定された比較データと上記レジスター（12）に保持されたデータとを比較して検証信号を出力する第 3 の比較器（16）を備えて構成される。

#### 【0011】

また、本発明のうち請求項 6 に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、一定回数を計数する第 1 のカウンタ（17）を備え、前記乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器（9）を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアする第 2 のカウンタ（18）を備え、第 2 のカウンタの出力データをデコードして各信号長ごとに出力するデコーダ（19）を備え、このデコーダの出力データを各信号長ごとにそれぞれカウントする複数の第 3 のカウンタ（20）を備え、第 1 のカウンタで計数された一定回数ごとに第 3 の各カウンタの出力データをそれぞれ保持する複数のレジスター（21）を備え、第 1 のカウンタで計数された一定回数ごとの信号と前記比較器の出力データとに基づいて前記各レジスターから検証データを出力するように制御する制御回路（22）を備えて構成される。

#### 【0012】

また、本発明のうち請求項 7 に係る発明は、上記レジスター（21）の出力データを選択して出力する選択回路（23）を付設して構成される。

#### 【0013】

また、本発明のうち請求項 8 に係る発明は、上記 1 ビット乱数発生装置（1）を複数個並列に接続し、これら 1 ビット乱数発生装置から出力された検証データをビットごとに選択して出力する選択回路（26）を付設して構成される。

#### 【0014】

また、本発明のうち請求項 9 に係る発明は、上記 1 ビット乱数発生装置（24

）を複数個並列に接続し、これら 1 ビット乱数発生装置から出力された検証信号をビットごとに選択して出力する選択回路（27）を付設して構成される。

#### 【0015】

また、本発明のうち請求項 10 に係る発明は、上記 1 ビット乱数発生装置（1、24）を有し、この 1 ビット乱数発生装置から出力された乱数データをシリアルデータからパラレルデータへ変換するシフトレジスター（31）を備え、一定のパラレルデータのビット長を計数するカウンタ（32）を備え、このカウンタで計数された周期ごとに前記シフトレジスターのパラレルデータを保持するレジスター（33）を備え、予め設定された確率上限データおよび確率下限データと前記レジスターに保持されたパラレルデータとを比較して確率信号を出力する比較器（34）を備えて構成される。

#### 【0016】

さらに、本発明のうち請求項 11 に係る発明は、上記多数ビット乱数発生装置（25）を有し、予め設定された確率上限データおよび確率下限データと前記多数ビット乱数発生装置から出力された乱数データとを比較して確率信号を出力する比較器（35）を備えて構成される。

#### 【0017】

これらの構成において、データ保持器の代表例として D タイプフリップフロップを挙げることができ、比較器の代表例としては排他的論理和素子（EXCLUSIVE-OR 素子）を挙げることができる。そして、こうした構成を採用することにより、乱数データの出現一様性を自ら検証することが可能となり、使用者が統計処理を行う必要がなくなるように作用する。

#### 【0018】

なお、括弧内の符号は図面において対応する要素を表す便宜的なものであり、したがって、本発明は図面上の記載に限定拘束されるものではない。このことは「特許請求の範囲」の欄についても同様である。

#### 【0019】

##### 【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

**【0020】**

図1は本発明に係る1ビット乱数発生装置の第1の実施形態を示す回路図である。

**【0021】**

この1ビット乱数発生装置1は、図1に示すように、乱数発生器2、第1のカウンタ3、第2のカウンタ4、レジスタ5および出力回路6から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号が第1のカウンタ3にも入力され、第1のカウンタ3は一定回数を計数して第2のカウンタ4およびレジスタ5に出力する。一方、第2のカウンタ4は、乱数発生器2から出力された乱数データの出現回数を計数して回数データを生成する。そして、レジスタ5は、第1のカウンタ3で計数された周期ごとに第2のカウンタ4の回数データを保持し、出力回路6は、レジスタ5に保持された回数データを検証データとしてシリアルまたはパラレルに出力する。

**【0022】**

したがって、この1ビット乱数発生装置1では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

**【0023】**

図2は本発明に係る1ビット乱数発生装置の第2の実施形態を示す回路図である。

**【0024】**

この1ビット乱数発生装置24は、図2に示すように、乱数発生器2、第1のカウンタ3、第2のカウンタ4、レジスタ5および比較器7から構成された検証信号出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号が第1のカウンタ3にも入力され、第1のカウンタ3は一定回数を計数する。一方、第2のカウンタ4は、乱数発生器2から出力された乱数データの出現回数を計数して回数データを生成する。そして、レジスタ5は

、第1のカウンター3で計数された周期ごとに第2のカウンター4の回数データを保持する。さらに、比較器7は、レジスタ5に保持されたデータと予め設定された上限比較データおよび下限比較データとを比較し、レジスタ5内のデータが上限比較データと下限比較データとの間にある場合には乱数データの出現一様性が高い旨の検証信号を出力し、それ以外の場合には乱数データの出現一様性が低い旨の検証信号を出力する。

#### 【0025】

したがって、この1ビット乱数発生装置24では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

#### 【0026】

図3は本発明に係る1ビット乱数発生装置の第3の実施形態を示す回路図である。

#### 【0027】

この1ビット乱数発生装置1は、乱数発生器2の出力が一様であれば“0”または“1”が出る確率は $1/2$ であるため、各々の数字が $k$ 回連続して出現する確率は $(1/2)^k$ であり、例えば30回連続して同じ数字が出現する確率は $1/1073741824$ （すなわち、ほとんどゼロ）となるので、もし30回連続して同じ数字が出現したら、この乱数発生器2は正常ではないと判断できるという考え方に基づくものである。

#### 【0028】

すなわち、この1ビット乱数発生装置1は、図3に示すように、乱数発生器2、Dタイプフリップフロップなどのデータ保持器8、排他的論理和素子などの比較器9、カウンタ10および出力回路6から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号および出力信号がデータ保持器8にも入力され、データ保持器8は、乱数発生器2から出力された前回の乱数データを保持して比較器9に出力する。また、比較器9には乱数発生器2の出力信号も入力され、比較器9は、乱数発生器2から出力された今回の乱数データとデータ保持器8に保持された前回の乱数データとを比較し

、両者が同一のときにはカウントアップ信号をカウンタ 10 に出力するとともに、両者が異なるときにはカウントクリア信号をカウンタ 10 に出力する。そして、カウンタ 10 には乱数発生器 2 の入力信号も入力され、カウンタ 10 はそのデータを出力回路 6 に出力し、出力回路 6 はそのデータを同一信号長の検証データとしてシリアルまたはパラレルに逐次出力する。

#### 【0029】

したがって、この 1 ビット乱数発生装置 1 では、出力された同一信号長の検証データによって、乱数の一様性を検証するための統計処理が容易になる。

#### 【0030】

図 4 は本発明に係る 1 ビット乱数発生装置の第 4 の実施形態を示す回路図である。

#### 【0031】

この 1 ビット乱数発生装置 1 は、図 4 に示すように、乱数発生器 2、D タイプフリップフロップなどのデータ保持器 8、排他的論理和素子などの第 1 の比較器 11、カウンタ 10、レジスタ 12、排他的論理和素子などの第 2 の比較器 13、制御回路 14 および出力回路 15 から構成された検証データ出力型であり、乱数発生器 2 に同期信号が入力されると、乱数発生器 2 から乱数データとして「1」または「0」が出力される。このとき、乱数発生器 2 の入力信号および出力信号がデータ保持器 8 にも入力され、データ保持器 8 は、乱数発生器 2 から出力された前回の乱数データを保持して第 1 の比較器 11 に出力する。また、第 1 の比較器 11 には乱数発生器 2 の出力信号も入力され、第 1 の比較器 11 は、乱数発生器 2 から出力された今回の乱数データとデータ保持器 8 に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンタ 10 に出力するとともに、両者が異なるときにはカウントクリア信号をカウンタ 10 に出力する。そして、カウンタ 10 には乱数発生器 2 の入力信号も入力され、カウンタ 10 はそのデータを第 2 の比較器 13 に出力し、第 2 の比較器 13 は、レジスタ 12 のデータとカウンタ 10 の出力データとを比較し、前者より後者の方が大きいときにはデータ上書き信号を制御回路 14 に出力するとともに、それ以外のときにはデータ保持信号を制御回路 14 に出力する。制御

回路 14 は、データ上書き信号を受けたときにはカウンタ 10 の出力データをレジスタ 12 に書き込むとともに、データ保持信号を受けたときにはレジスタ 12 のデータを保持するように制御し、出力回路 15 は、レジスタ 12 に保持されたデータを最長の同一信号長の検証データとしてシリアルまたはパラレルに逐次出力する。

#### 【0032】

したがって、この 1 ビット乱数発生装置 1 では、出力された最長の同一信号長の検証データによって、乱数の一様性を検証するための統計処理が容易になる。

#### 【0033】

図 5 は本発明に係る 1 ビット乱数発生装置の第 5 の実施形態を示す回路図である。

#### 【0034】

この 1 ビット乱数発生装置 24 は、図 5 に示すように、乱数発生器 2、D タイプフリップフロップなどのデータ保持器 8、排他的論理和素子などの第 1 の比較器 11、カウンタ 10、レジスタ 12、排他的論理和素子などの第 2 の比較器 13、制御回路 14 および排他的論理和素子などの第 3 の比較器 16 から構成された検証信号出力型であり、乱数発生器 2 に同期信号が入力されると、乱数発生器 2 から乱数データとして「1」または「0」が出力される。このとき、乱数発生器 2 の入力信号および出力信号がデータ保持器 8 にも入力され、データ保持器 8 は、乱数発生器 2 から出力された前回の乱数データを保持して第 1 の比較器 11 に出力する。また、第 1 の比較器 11 には乱数発生器 2 の出力信号も入力され、第 1 の比較器 11 は、乱数発生器 2 から出力された今回の乱数データとデータ保持器 8 に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンタ 10 に出力するとともに、両者が異なるときにはカウントクリア信号をカウンタ 10 に出力する。そして、カウンタ 10 には乱数発生器 2 の入力信号も入力され、カウンタ 10 はそのデータを第 2 の比較器 13 に出力し、第 2 の比較器 13 は、レジスタ 12 のデータとカウンタ 10 の出力データとを比較し、前者より後者の方が大きいときにはデータ上書き信号を制御回路 14 に出力するとともに、それ以外のときにはデータ保持信号を制



御回路 14 に出力する。制御回路 14 は、データ上書き信号を受けたときにはカウンタ 10 の出力データをレジスタ 12 に書き込むとともに、データ保持信号を受けたときにはレジスタ 12 のデータを保持するように制御し、第 3 の比較器 16 は、レジスタ 12 に保持されたデータと予め設定された比較データとを比較して最長の同一信号長の検証信号を逐次出力する。

#### 【0035】

したがって、この 1 ビット乱数発生装置 24 では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

#### 【0036】

図 6 は本発明に係る 1 ビット乱数発生装置の第 6 の実施形態を示す回路図である。

#### 【0037】

この 1 ビット乱数発生装置 1 は、図 6 に示すように、乱数発生器 2、D タイプフリップフロップなどのデータ保持器 8、排他的論理和素子などの比較器 9、第 1 のカウンタ 17、第 2 のカウンタ 18、デコーダ 19、複数個 ( $n$  個) の第 3 のカウンタ 20、複数個 ( $n$  個) のレジスタ 21 および制御回路 22 から構成された検証データ出力型であり、乱数発生器 2 に同期信号が入力されると、乱数発生器 2 から乱数データとして「1」または「0」が出力される。このとき、第 1 のカウンタ 17 が計数する一定回数での各同一信号長 ( $1 \sim n$ ) の出現率をカウントし、第 1 のカウンタ 17 が計数する一定回数ごとにレジスタ 21 に書き込み、各同一信号長の分布を逐次出力する。

#### 【0038】

すなわち、乱数発生器 2 の入力信号および出力信号がデータ保持器 8 にも入力され、データ保持器 8 は、乱数発生器 2 から出力された前回の乱数データを保持して比較器 9 に出力する。また、比較器 9 には乱数発生器 2 の出力信号も入力され、比較器 9 は、乱数発生器 2 から出力された今回の乱数データとデータ保持器 8 に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号を制御回路 22 に出力するとともに、両者が異なるときにはカウントクリア信号を制御回路 22 に出力する。一方、乱数発生器 2 の入力信号は第 1 のカ

ウンター 17 および制御回路 22 にも入力され、第 1 のカウンタ 17 は一定回数を計数して制御回路 22 に出力する。さらに、乱数発生器 2 の入力信号は第 2 のカウンタ 18 にも入力され、第 2 のカウンタ 18 は、比較器 9 からカウントアップ信号を受けたときにはカウントアップしてデコーダ 19 に出力するとともに、比較器 9 からカウントクリア信号を受けたときにはカウントクリアしてデコーダ 19 に出力する。これを受けてデコーダ 19 は、第 2 のカウンタ 18 の出力データをデコードして各信号長ごとに第 3 の各カウンタ 20 へ出力し、各カウンタ 20 はこの出力データをカウントして各レジスタ 21 に出力する。そして、各レジスタ 21 は、制御回路 22 による制御下で、比較器 9 の出力データと第 1 のカウンタ 17 で計数された一定回数ごとの信号とに基づいて同一信号長の検証データをシリアルまたはパラレルに逐次出力する。

#### 【0039】

したがって、この 1 ビット乱数発生装置 1 では、出力された各カウント数（検証データ）によって、乱数の一様性を検証するための統計処理が容易になる。

#### 【0040】

図 7 は本発明に係る 1 ビット乱数発生装置の第 7 の実施形態を示す回路図である。

#### 【0041】

この 1 ビット乱数発生装置 1 は、図 7 に示すように、乱数発生器 2、D タイプフリップフロップなどのデータ保持器 8、排他的論理和素子などの比較器 9、第 1 のカウンタ 17、第 2 のカウンタ 18、デコーダ 19、複数個（ $n$  個）の第 3 のカウンタ 20、複数個（ $n$  個）のレジスタ 21、制御回路 22 および選択回路 23 から構成された検証データ出力型であり、乱数発生器 2 に同期信号が入力されると、乱数発生器 2 から乱数データとして「1」または「0」が出力される。このとき、第 1 のカウンタ 17 が計数する一定回数での各同一信号長（ $1 \sim n$ ）の出現率をカウントし、第 1 のカウンタ 17 が計数する一定回数ごとにレジスタ 21 に書き込み、各同一信号長の分布を外部からの選択データで選択できる選択回路 23 にて逐次出力する。

#### 【0042】

すなわち、乱数発生器 2 の入力信号および出力信号がデータ保持器 8 にも入力され、データ保持器 8 は、乱数発生器 2 から出力された前回の乱数データを保持して比較器 9 に出力する。また、比較器 9 には乱数発生器 2 の出力信号も入力され、比較器 9 は、乱数発生器 2 から出力された今回の乱数データとデータ保持器 8 に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号を制御回路 22 に出力するとともに、両者が異なるときにはカウントクリア信号を制御回路 22 に出力する。一方、乱数発生器 2 の入力信号は第 1 のカウンタ 17 および制御回路 22 にも入力され、第 1 のカウンタ 17 は一定回数を計数して制御回路 22 に出力する。さらに、乱数発生器 2 の入力信号は第 2 のカウンタ 18 にも入力され、第 2 のカウンタ 18 は、比較器 9 からカウントアップ信号を受けたときにはカウントアップしてデコーダ 19 に出力するとともに、比較器 9 からカウントクリア信号を受けたときにはカウントクリアしてデコーダ 19 に出力する。これを受けてデコーダ 19 は、第 2 のカウンタ 18 の出力データをデコードして各信号長ごとに第 3 の各カウンタ 20 へ出力し、各カウンタ 20 はこの出力データをカウントして各レジスタ 21 に出力する。そして、各レジスタ 21 は、制御回路 22 による制御下で、比較器 9 の出力データと第 1 のカウンタ 17 で計数された一定回数ごとの信号とに基づいて同一信号長の検証データを選択回路 23 にシリアルまたはパラレルに逐次出力する。さらに、選択回路 23 に外部から選択データが入力されると、選択回路 23 はレジスタ 21 の出力データをその選択データに基づいて適宜選択して出力する。

#### 【0043】

したがって、この 1 ビット乱数発生装置 1 では、出力された同一信号長の分布データによって、乱数の一様性を検証するための統計処理が容易になる。

#### 【0044】

図 8 は本発明に係る多数ビット乱数発生装置の第 1 の実施形態を示す回路図である。

#### 【0045】

この多数ビット乱数発生装置 25 は、図 8 に示すように、上述した検証データ

出力型の 1 ビット乱数発生装置 1 を複数個（n 個）並列に接続し、これに選択回路 26 を付設したものであり、選択回路 26 に外部から選択データが入力されると、選択回路 26 は、1 ビット乱数発生装置 1 から出力された検証データをその選択データに基づいてビットごとに選択して出力する。

#### 【0046】

したがって、この多数ビット乱数発生装置 25 では、出力された一様性検証データによって、乱数の一様性を検証するための統計処理が容易になる。

#### 【0047】

図 9 は本発明に係る多数ビット乱数発生装置の第 2 の実施形態を示す回路図である。

#### 【0048】

この多数ビット乱数発生装置 25 は、図 9 に示すように、上述した検証信号出力型の 1 ビット乱数発生装置 24 を複数個（n 個）並列に接続し、これに選択回路 27 を付設したものであり、選択回路 27 に外部から選択データが入力されると、選択回路 27 は、1 ビット乱数発生装置 24 から出力された検証信号をその選択データに基づいてビットごとに選択して出力する。

#### 【0049】

したがって、この多数ビット乱数発生装置 25 では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

#### 【0050】

図 10 は本発明に係る確率発生装置の第 1 の実施形態を示す回路図である。

#### 【0051】

この確率発生装置 30 は、図 10 に示すように、上述した検証データ出力型の 1 ビット乱数発生装置 1、シフトレジスタ 31、カウンタ 32、レジスタ 33 および比較器 34 から構成されており、1 ビット乱数発生装置 1 から出力された乱数データはシフトレジスタ 31 に入力され、シフトレジスタ 31 はこの乱数データをシリアルデータからパラレルデータへ変換してレジスタ 33 に出力する。一方、1 ビット乱数発生装置 1 の入力信号はカウンタ 32 にも

入力され、カウンタ 32 は一定の平行データのビット長を計数してレジスタ 33 に出力する。すると、レジスタ 33 は、カウンタ 32 で計数された周期ごとにシフトレジスタ 31 の平行データを保持する。そして、比較器 34 は、レジスタ 33 に保持されたデータと予め設定された確率上限データおよび確率下限データとを比較し、レジスタ 33 内のデータが確率上限データと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

#### 【0052】

したがって、この確率発生装置 30 では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

#### 【0053】

図 11 は本発明に係る確率発生装置の第 2 の実施形態を示す回路図である。

#### 【0054】

この確率発生装置 30 は、図 11 に示すように、上述した検証信号出力型の 1 ビット乱数発生装置 24、シフトレジスタ 31、カウンタ 32、レジスタ 33 および比較器 34 から構成されており、1 ビット乱数発生装置 24 から出力された乱数データはシフトレジスタ 31 に入力され、シフトレジスタ 31 はこの乱数データをシリアルデータから平行データへ変換してレジスタ 33 に出力する。一方、1 ビット乱数発生装置 24 の入力信号はカウンタ 32 にも入力され、カウンタ 32 は一定の平行データのビット長を計数してレジスタ 33 に出力する。すると、レジスタ 33 は、カウンタ 32 で計数された周期ごとにシフトレジスタ 31 の平行データを保持する。そして、比較器 34 は、レジスタ 33 に保持されたデータと予め設定された確率上限データおよび確率下限データとを比較し、レジスタ 33 内のデータが確率上限データと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

#### 【0055】

したがって、この確率発生装置 30 では、使用者が面倒で煩雑な統計処理を行

わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

#### 【0056】

図12は本発明に係る確率発生装置の第3の実施形態を示す回路図、図13は本発明に係る確率発生装置の第4の実施形態を示す回路図である。

#### 【0057】

これらの確率発生装置30は、図12および図13に示すように、上述した多数ビット乱数発生装置25および比較器35から構成されており、多数ビット乱数発生装置25から出力された乱数データ（パラレルデータ）は比較器35に入力され、比較器35は、この乱数データと予め設定された確率上限データおよび確率下限データとを比較し、乱数データが確率上限データと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

#### 【0058】

したがって、この確率発生装置30では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

#### 【0059】

##### 【発明の効果】

以上説明したように、本発明のうち請求項1～7に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な1ビット乱数発生装置を提供することができる。

#### 【0060】

また、本発明のうち請求項8、9に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な多数ビット乱数発生装置を提供することができる。

#### 【0061】

さらに、本発明のうち請求項 10、11に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な確率発生装置を提供することができる。

**【図面の簡単な説明】**

**【図 1】**

本発明に係る 1 ビット乱数発生装置の第 1 の実施形態を示す回路図である。

**【図 2】**

本発明に係る 1 ビット乱数発生装置の第 2 の実施形態を示す回路図である。

**【図 3】**

本発明に係る 1 ビット乱数発生装置の第 3 の実施形態を示す回路図である。

**【図 4】**

本発明に係る 1 ビット乱数発生装置の第 4 の実施形態を示す回路図である。

**【図 5】**

本発明に係る 1 ビット乱数発生装置の第 5 の実施形態を示す回路図である。

**【図 6】**

本発明に係る 1 ビット乱数発生装置の第 6 の実施形態を示す回路図である。

**【図 7】**

本発明に係る 1 ビット乱数発生装置の第 7 の実施形態を示す回路図である。

**【図 8】**

本発明に係る多数ビット乱数発生装置の第 1 の実施形態を示す回路図である。

**【図 9】**

本発明に係る多数ビット乱数発生装置の第 2 の実施形態を示す回路図である。

**【図 10】**

本発明に係る確率発生装置の第 1 の実施形態を示す回路図である。

**【図 11】**

本発明に係る確率発生装置の第 2 の実施形態を示す回路図である。

**【図 12】**

本発明に係る確率発生装置の第 3 の実施形態を示す回路図である。

## 【図 1 3】

本発明に係る確率発生装置の第 4 の実施形態を示す回路図である。

## 【符号の説明】

- 1 …… 1 ビット乱数発生装置
- 2 …… 乱数発生器
- 3 …… 第 1 のカウンタ
- 4 …… 第 2 のカウンタ
- 5 …… レジスタ
- 6 …… 出力回路
- 7 …… 比較器
- 8 …… データ保持器
- 9 …… 比較器
- 1 0 …… カウンタ
- 1 1 …… 第 1 の比較器
- 1 2 …… レジスタ
- 1 3 …… 第 2 の比較器
- 1 4 …… 制御回路
- 1 5 …… 出力回路
- 1 6 …… 第 3 の比較器
- 1 7 …… 第 1 のカウンタ
- 1 8 …… 第 2 のカウンタ
- 1 9 …… デコーダ
- 2 0 …… 第 3 のカウンタ
- 2 1 …… レジスタ
- 2 2 …… 制御回路
- 2 3 …… 選択回路
- 2 4 …… 1 ビット乱数発生装置
- 2 5 …… 多数ビット乱数発生装置
- 2 6 …… 選択回路



2 7 .....選択回路

3 0 .....確率発生装置

3 1 .....シフトレジスター

3 2 .....カウンタ

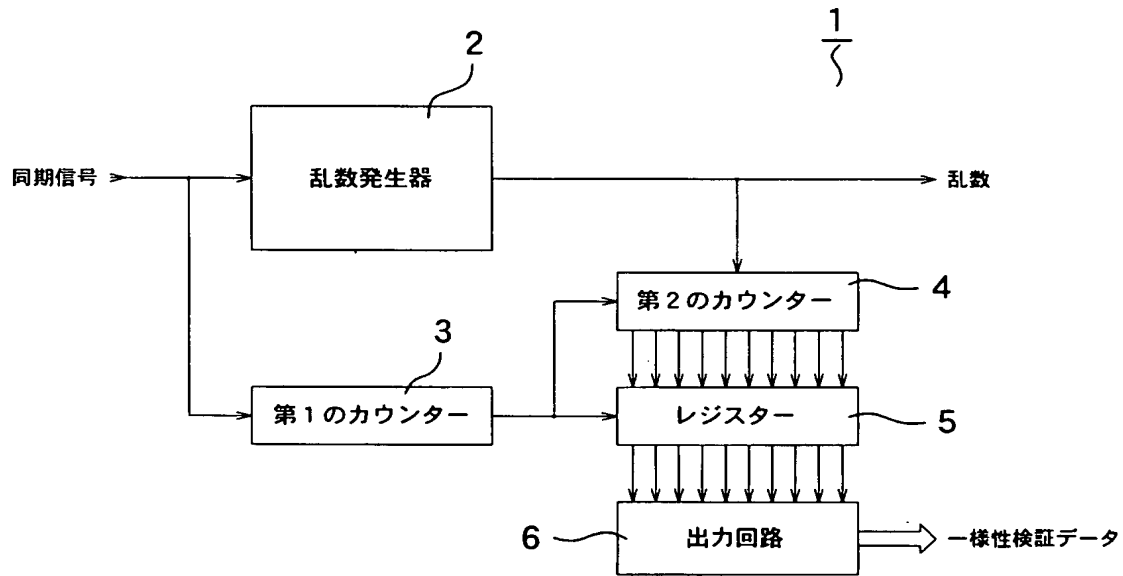
3 3 .....レジスター

3 4 .....比較器

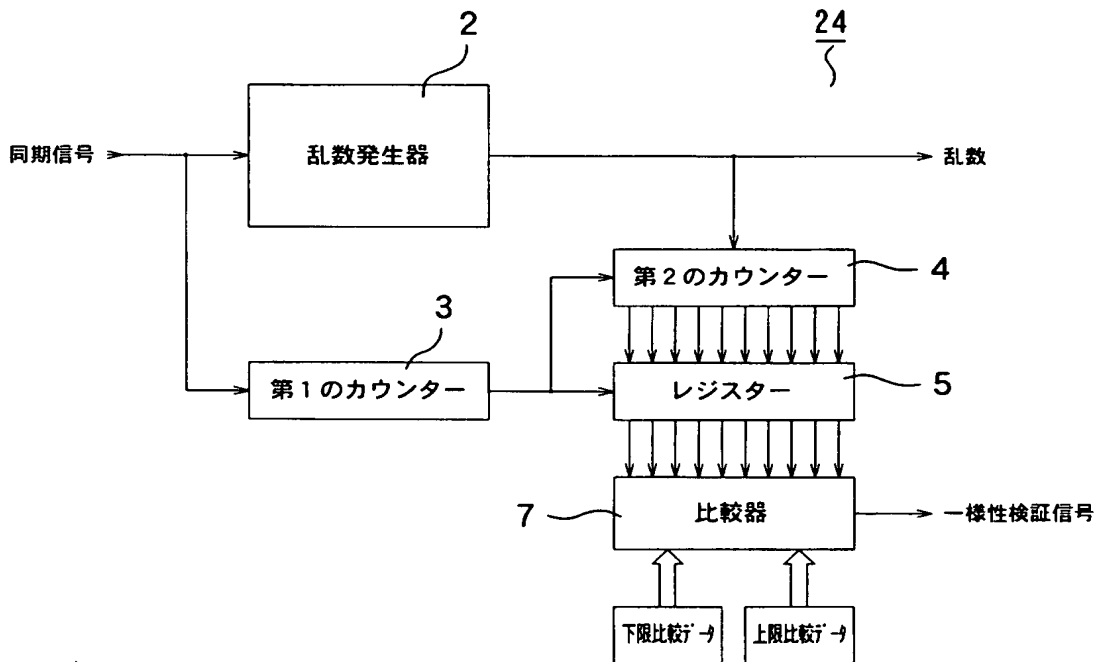
3 5 .....比較器

【書類名】 図面

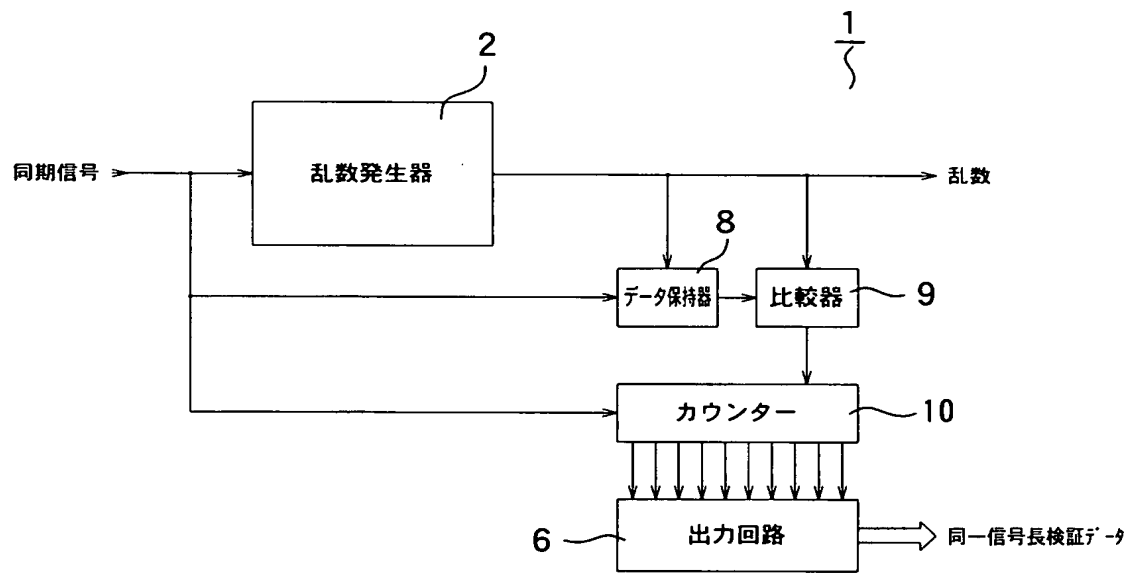
【図 1】



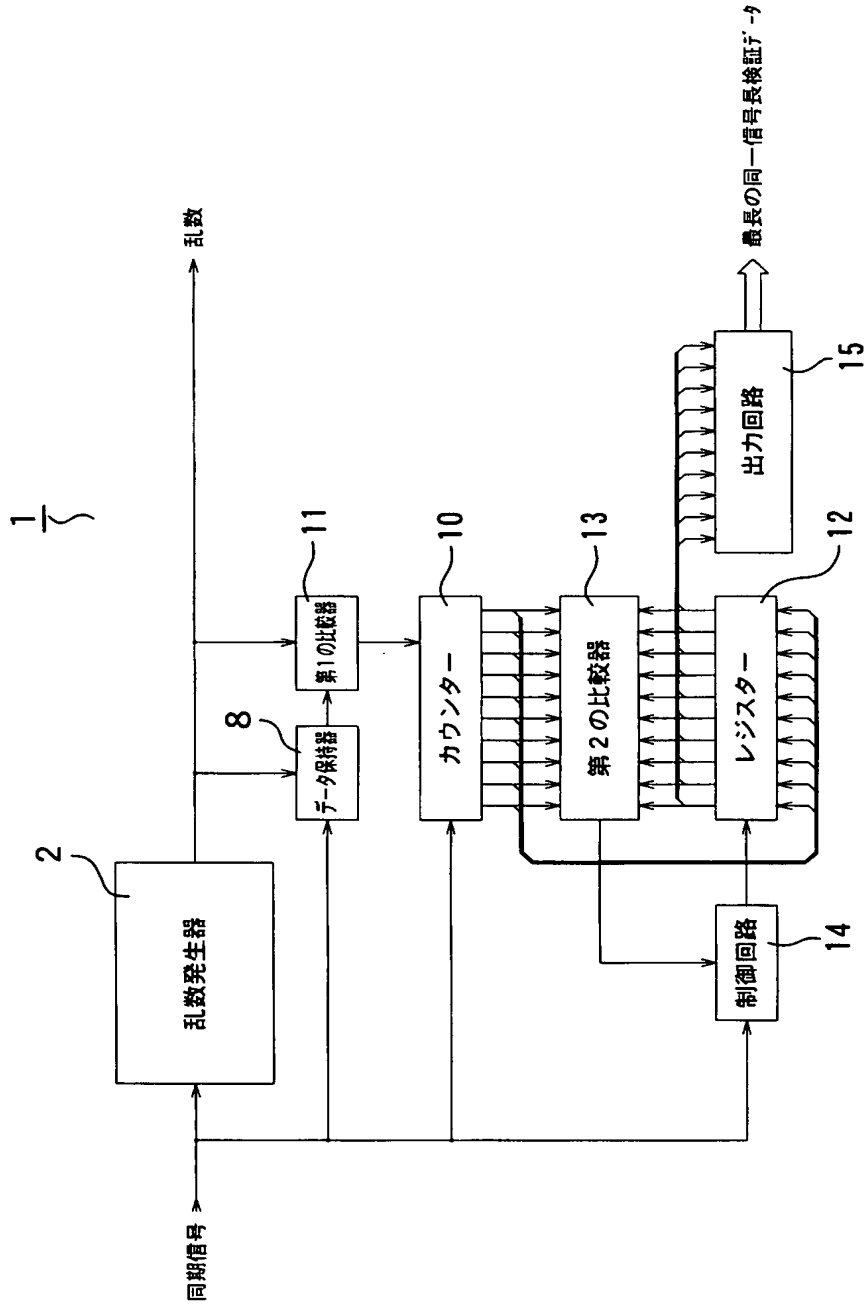
【図 2】



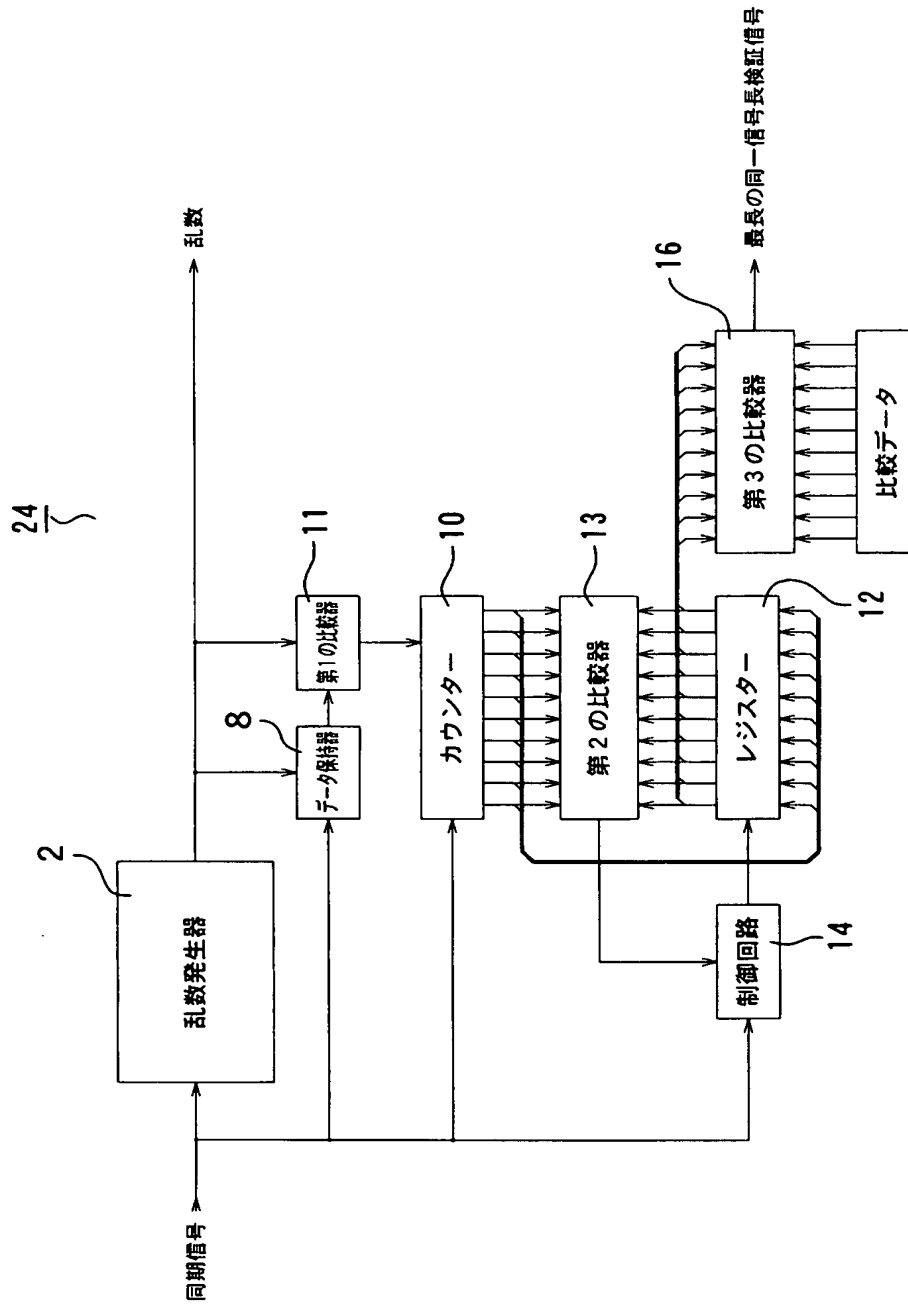
【図 3】



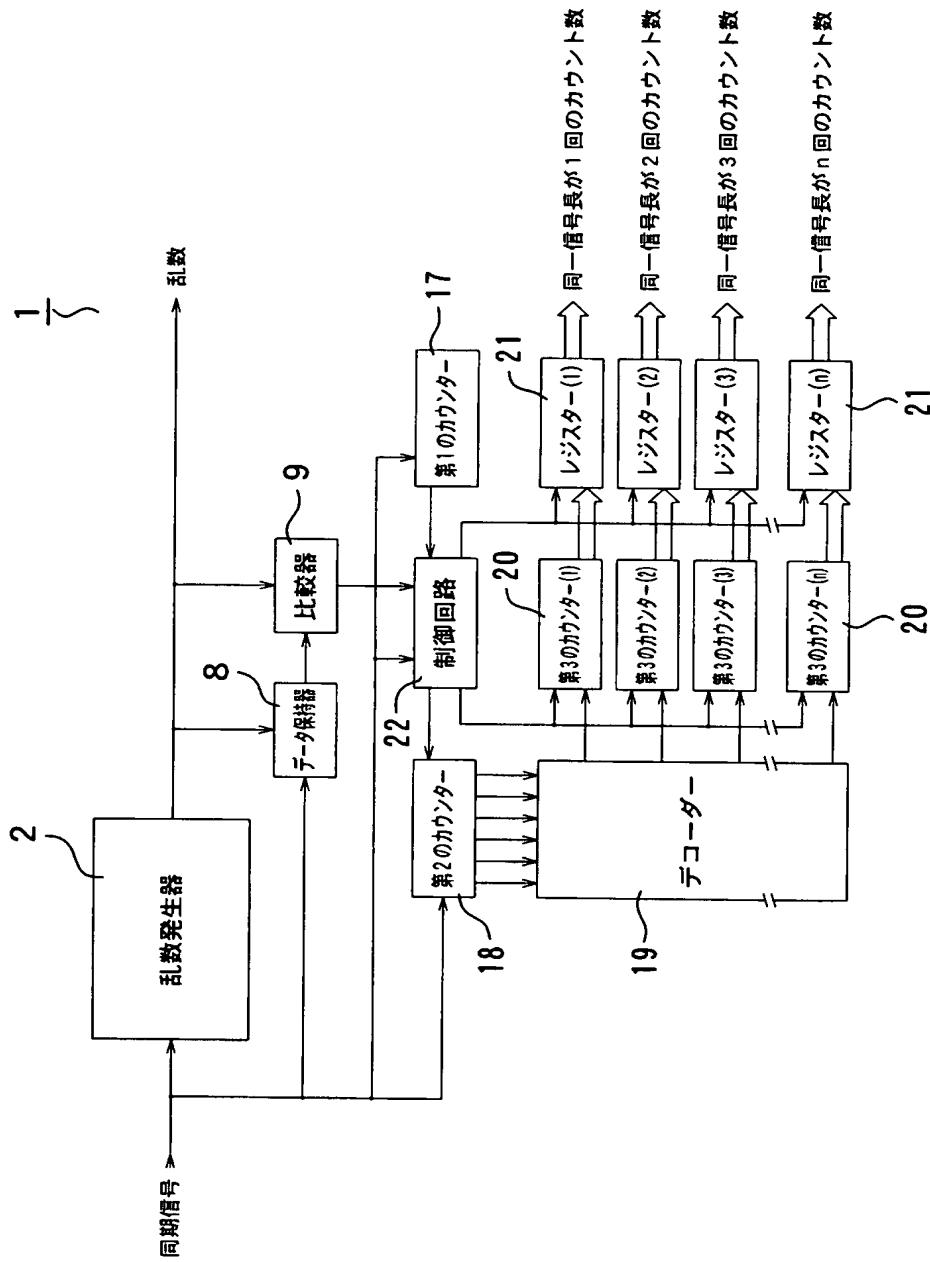
【図 4】



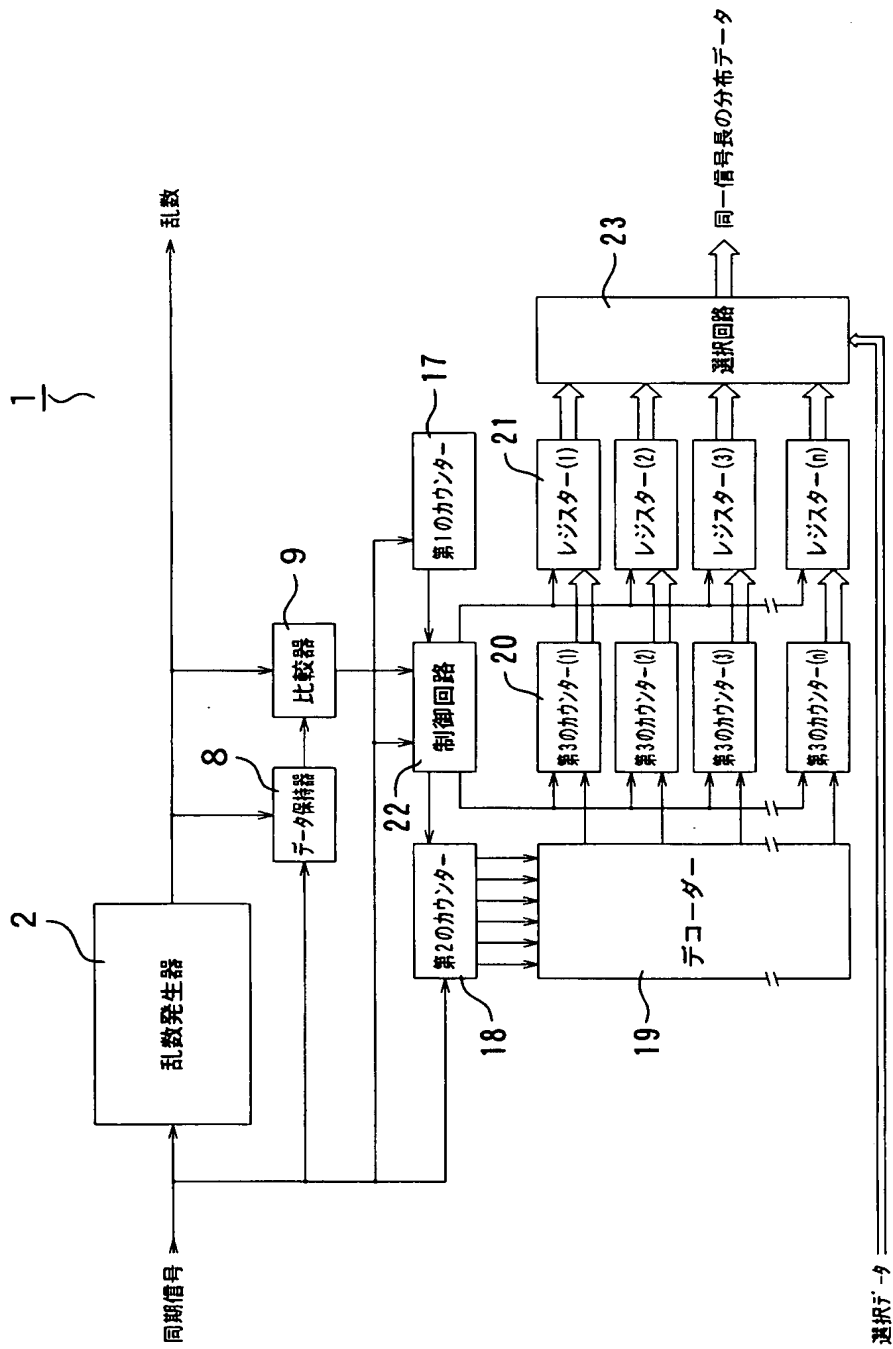
【図 5】



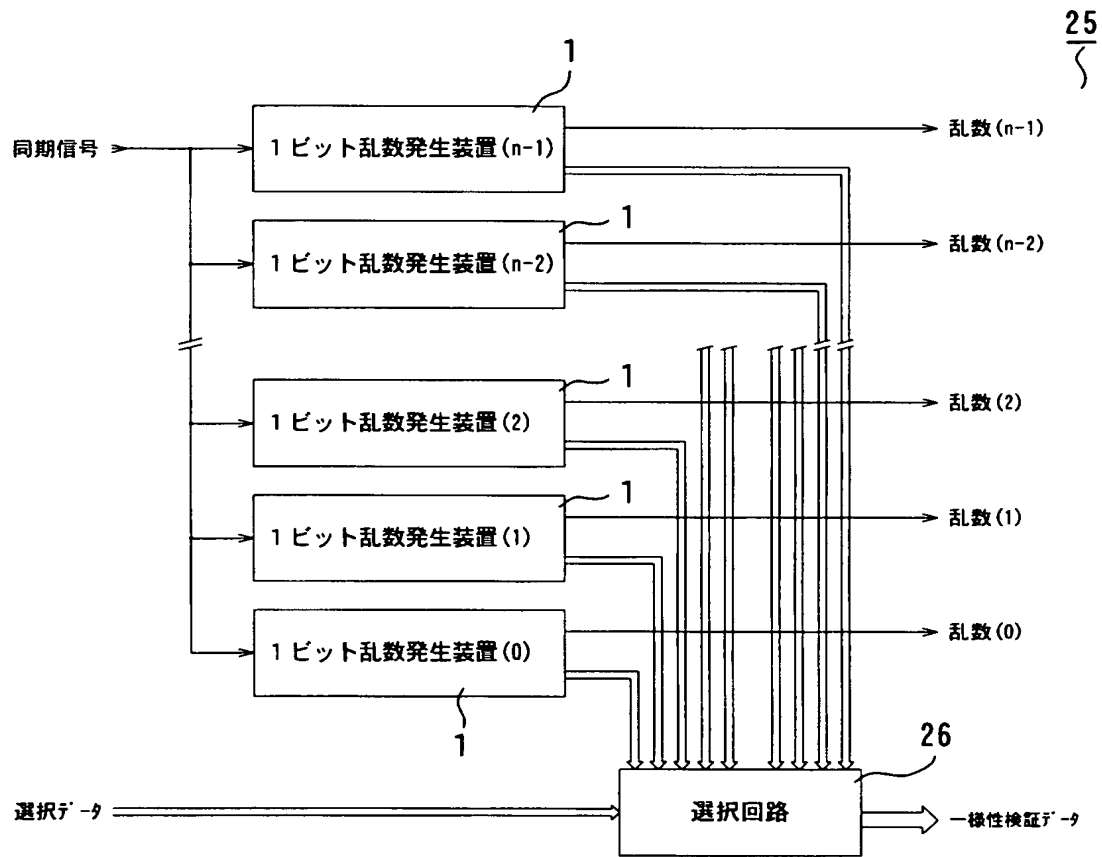
【図 6】



【図 7】

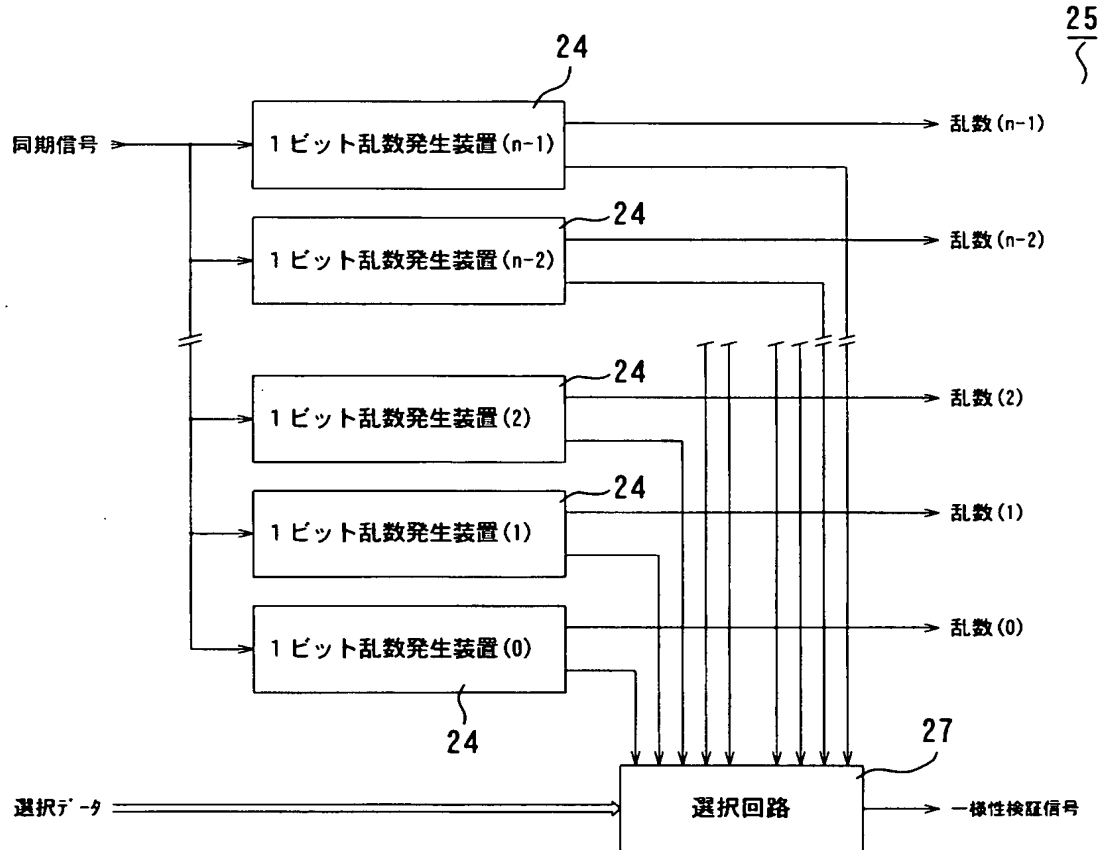


【図 8】

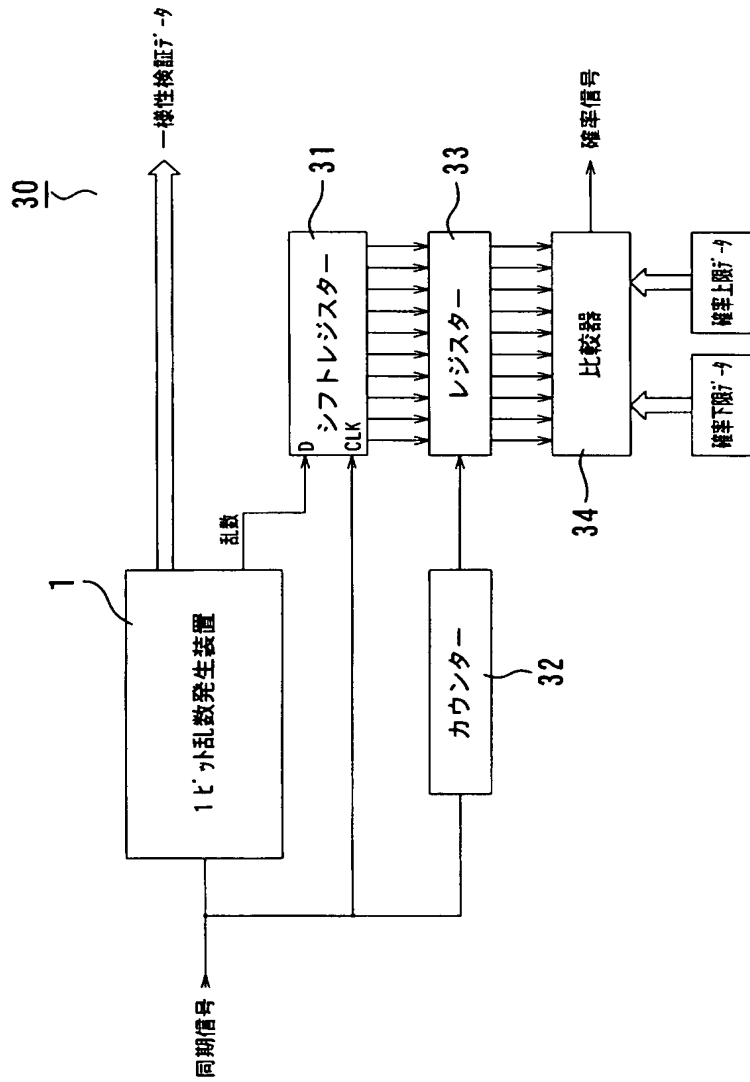




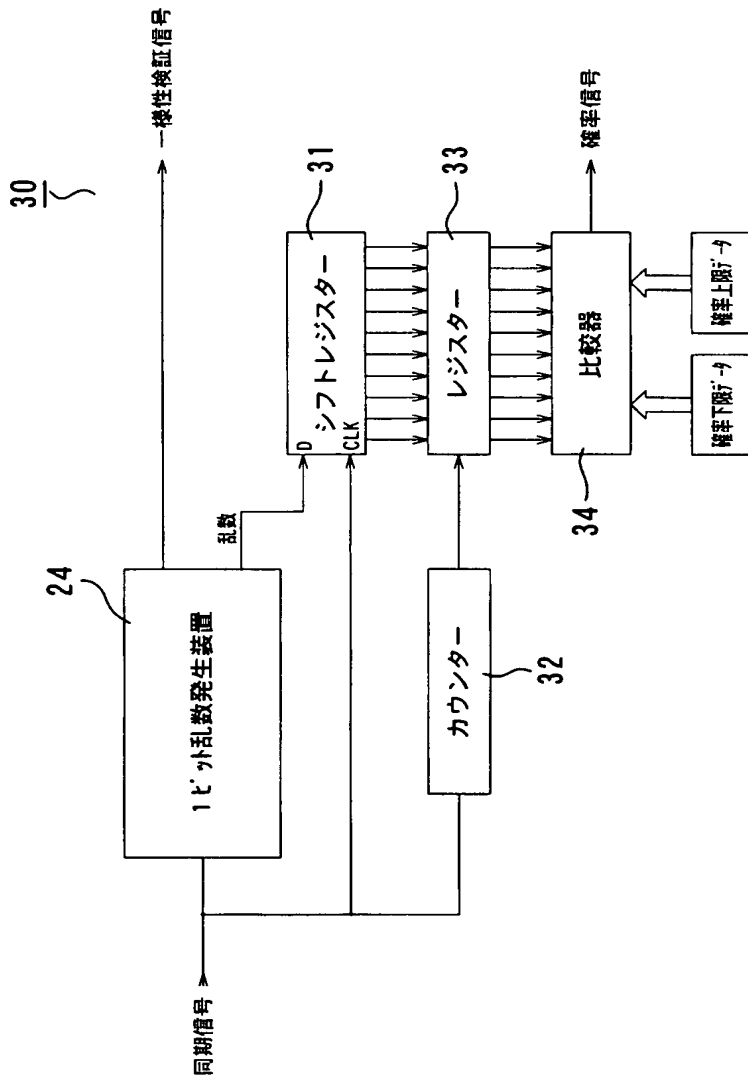
【図 9】



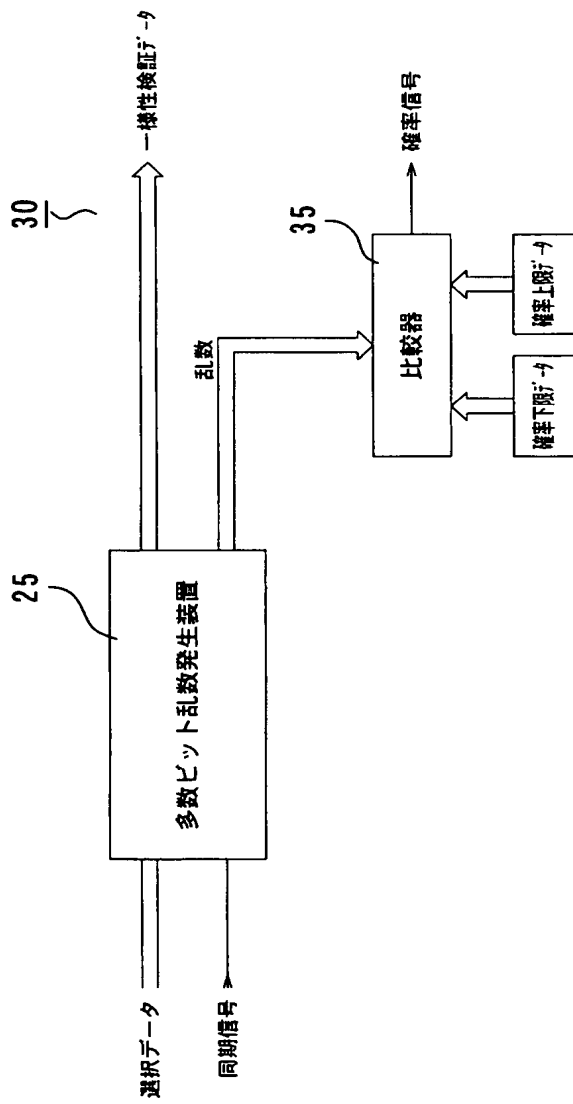
【図 10】



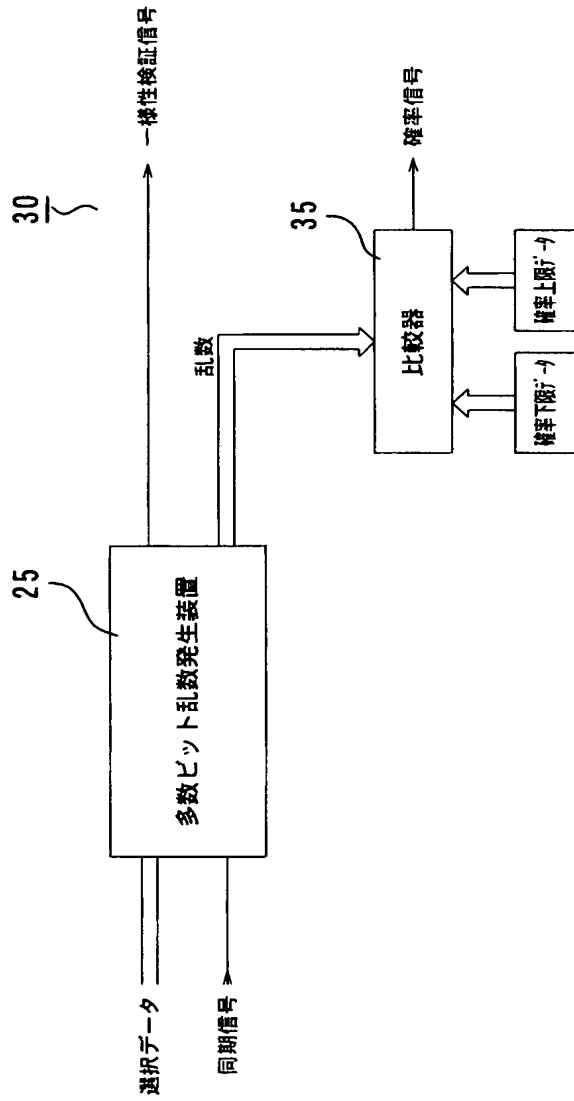
【図 11】



【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 科学技術計算などに利用される乱数発生装置および確率発生装置において、乱数データの出現一様性を手軽に検証して信頼性を高める。

【解決手段】 乱数データとして「1」と「0」を出力する乱数発生器 2 に、一定回数を計数する第 1 のカウンター 3 と、乱数データの出現回数を計数して回数データを生成する第 2 のカウンター 4 とを備える。第 1 のカウンター 3 で計数された周期ごとに第 2 のカウンター 4 の回数データをレジスター 5 が保持し、レジスター 5 に保持された回数データを出力回路 6 が検証データとして出力する。これにより、乱数データの出現一様性を自ら検証でき、使用者が統計処理を行う必要がなくなる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 1 - 2 1 6 7 0 4
受付番号	5 0 1 0 1 0 4 9 6 1 8
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 3 年 7 月 1 8 日

< 認定情報・付加情報 >

【提出日】	平成13年 7月17日
-------	-------------

次頁無

【書類名】 出願人名義変更届（一般承継）  
【整理番号】 IP01397  
【あて先】 特許庁長官 殿  
【事件の表示】  
    【出願番号】 特願2001-216704  
【承継人】  
    【識別番号】 000237721  
    【氏名又は名称】 エフ・ディー・ケイ株式会社  
【承継人代理人】  
    【識別番号】 100067046  
    【弁理士】  
    【氏名又は名称】 尾股 行雄  
    【電話番号】 03-3543-0036  
【提出物件の目録】  
    【包括委任状番号】 0014478  
    【物件名】 閉鎖事項全部証明書 1  
    【援用の表示】 特願 2 0 0 1 - 1 7 0 6 5 2  
    【物件名】 履歴事項全部証明書 1  
    【援用の表示】 特願 2 0 0 1 - 1 7 0 6 5 2  
【プルーフの要否】 要



認定・付加情報

特許出願の番号	特願 2001-216704
受付番号	50200888594
書類名	出願人名義変更届（一般承継）
担当官	井筒 セイ子 1354
作成日	平成14年 7月24日

<認定情報・付加情報>

【提出日】	平成14年 6月19日
-------	-------------

次頁無

特願 2 0 0 1 - 2 1 6 7 0 4

出 願 人 履 歴 情 報

識別番号

[ 3 9 0 0 2 2 7 9 2 ]

1. 変更年月日

1 9 9 0 年 1 1 月 1 3 日

[変更理由]

新規登録

住 所

東京都港区新橋 5 丁目 3 6 番 1 1 号

氏 名

いわき電子株式会社

特願 2 0 0 1 - 2 1 6 7 0 4

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 2 3 7 7 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区新橋 5 丁目 3 6 番 1 1 号

氏 名

富士電気化学株式会社

2. 変更年月日

2 0 0 1 年 1 月 1 6 日

[変更理由]

名称変更

住 所

東京都港区新橋 5 丁目 3 6 番 1 1 号

氏 名

エフ・ディー・ケイ株式会社



(Translation)

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: July 18, 2001  
Application Number: No. 2001-217710  
Applicant: FDK Corporation

Date: August 7, 2003  
Commissioner, Patent Office Yasuo IMAI (Seal)

Certificate No. 2003-3063566